日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　４月　８日
出願番号 Application Number:	特願２００４－１１４３３０
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－１１４３３０
出願人 Applicant(s):	松下電器産業株式会社

２００５年　４月２０日

特許庁長官
Commissioner,
Japan Patent Office

小川

【書類名】　特許願
【整理番号】　2968260006
【あて先】　特許庁長官　殿
【国際特許分類】　G06K 15/00
【発明者】
【住所又は居所】　広島県東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内
【氏名】　江原　裕美
【発明者】
【住所又は居所】　広島県東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内
【氏名】　植田　栄治
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100105175
【弁理士】
【氏名又は名称】　山広　宗則
【電話番号】　082-222-9109
【選任した代理人】
【識別番号】　100105197
【弁理士】
【氏名又は名称】　岩本　牧子
【手数料の表示】
【予納台帳番号】　043775
【納付金額】　16,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0215016

【書類名】特許請求の範囲
【請求項１】
複数のサービスを提供可能な半導体メモリカードにおいて、
複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル情報管理手段と、
前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段と、
を備えたことを特徴とする、半導体メモリカード。
【請求項２】
前記セキュリティレベル情報取得手段により取得した、前記セキュリティレベル情報を出力するセキュリティレベル情報出力手段と、
をさらに備えたことを特徴とする、請求項１記載の半導体メモリカード。
【請求項３】
前記セキュリティレベル情報取得手段で取得した前記セキュリティレベル情報を比較するセキュリティレベル情報比較手段と、
前記セキュリティレベル情報比較手段で比較した結果を基に、所定のデータ操作処理を行うデータ操作手段と、
をさらに備えたことを特徴とする、請求項１記載の半導体メモリカード。
【請求項４】
前記セキュリティレベル情報は、前記サービスにおいて取り扱うデータに対する暗号化条件であることを特徴とする、請求項１記載の半導体メモリカード。
【請求項５】
前記セキュリティレベル情報は、前記サービスを提供するアプリケーションのバージョン番号を含むことを特徴とする、請求項１記載の半導体メモリカード。
【請求項６】
前記セキュリティレベル情報比較手段は、さらに、比較結果を保存し、
前記セキュリティレベル情報取得手段は、前記保存されたセキュリティレベル情報が存在する場合、該セキュリティレベル情報を取得することを特徴とする、請求項１記載の半導体メモリカード
【請求項７】
複数のサービスを提供可能な半導体メモリカードに格納されたデータを処理する方法であって、
複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、
前記セキュリティレベル情報を取得することを特徴とする、半導体メモリカード処理方法。
【請求項８】
複数のサービスを提供可能な半導体メモリカードにおいて、該半導体メモリカード内部のＣＰＵにより実行される制御プログラムであって、
複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、
前記セキュリティレベル情報を取得することを特徴とする、半導体メモリカード処理プログラム。
【請求項９】
複数のサービスを提供可能な半導体メモリカードにおいて用いられる、集積回路であって、
複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル情報管理手段と、
前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段とを備えること特徴とする集積回路。

【書類名】明細書
【発明の名称】半導体メモリカード、半導体メモリカード処理方法、半導体メモリカード処理プログラム、および集積回路
【技術分野】
【０００１】
本発明は複数のサービスを搭載可能な半導体メモリカードに関し、特に格納内容のセキュリティを保証し、情報の漏洩を防ぐ事を目的とした半導体メモリカード、半導体メモリカード処理方法及び半導体メモリカード処理プログラム、および集積回路に関するものである。
【背景技術】
【０００２】
現在半導体メモリカードはマスメディアや金融機関、国、自治体など様々な分野から注目を集めている。その理由として、格納データの保護機能が挙げられる。格納データの保護機能を持った半導体メモリカードの代表としてＳＤメモリカードやＩＣカードがある。
図２は一般的なＩＣカードの内部構造を示す図である。従来、クレジットカードをはじめ多くの磁気カードがＩＣカードへ転換されてきている。その理由として、ＩＣカードは半導体メモリを備えるカードであり、プログラムを格納するＲＯＭ２０３、プログラム実行の際に用いられるデータを一時的に格納するＲＡＭ２０２、ＲＯＭ２０３に記憶されたプログラムに従って各種コマンド処理等の制御処理を行うＣＰＵ２０１、外部からダウンロードされたプログラムを格納する書き換え可能なＥＥＰＲＯＭ２０４で構成されている。ＩＣカードは磁気カードに比べて記憶容量が大きいことはもとより、格納される個人情報等のセキュリティ機能の向上がなされていることが特徴として挙げられる。
【０００３】
ところで、このＩＣカードは通常一枚のカード内に電子マネー等の単一のサービスのみを備えて用いられてきたが、近年のＩＣカードにおけるメモリの記憶容量やＣＰＵの処理速度向上にともない、複数のサービスを一枚のＩＣカードで実現するものが提案されてきている。これにより、利用者が複数枚の異なるＩＣカードを所持する必要をなくし、一枚のＩＣカードで異なる様々なサービスを享受することが可能となってきている。
このように、複数のサービスに対応するＩＣカードは、複数のアプリケーションを備えているので、該ＩＣカードを以後マルチアプリケーション対応のＩＣカードと呼び、以後の説明において、単にＩＣカードを示す場合はマルチアプリケーション対応のＩＣカードを意味するものとする。
【０００４】
図３は、上述したＩＣカードにおけるソフトウエェア構成を示す図である。ＩＣカードのソフトウェアはレイヤ構造をもち、このレイヤ構造では最下位層にアプリケーション用メモリ領域３１０があり、この上位層にＯＳ３１１、最上位層に複数のアプリケーションが存在し、例えばクライアントＥＣアプリケーション３０１、クライアントＥＣアプリケーション３０２あるいはクライアント公共アプリケーション３０３がある。一般のＩＣカードで複数のサービスに対応するためには、上記のごとく一枚のＩＣカードに複数のアプリケーションを備え、かつ各アプリケーションはＯＳ３１１のファイヤウォール機能により、互いのアプリケーション用メモリ領域３１０を侵害することはないようになっている。また、従来これらのアプリケーションは互いに独立しており、連携する手段も存在していない。
そのため、例えば、ある電子マネーサービスが保持している電子マネーをサービス提供会社が異なる交通系サービスの電子マネーに移行する場合など、カード外のホスト端末のアプリケーションによりホストにデータを読み出し、ホスト側において、他のアプリケーション等を仲介してデータ交換の可否決定と実行をする必要がある。
【特許文献１】特許第２０８６９２４号公報
【発明の開示】
【発明が解決しようとする課題】

【０００５】
上述したように、従来の技術では、外部アプリケーションがカード内のデータおよび、データの暗号化情報を一旦カード外部へ読み出し、データ交換可否を決定し、演算や書き込みの処理を行うため、暗号化情報が外部に漏洩する危険性があり、さらに電子マネーなどの重要なデータも外部に漏洩、改竄される危険が発生するという課題を有していた。
本発明は、前記従来の課題を解決するもので、ＩＣカードに代表される半導体メモリカードに格納されている異なるサービス間のデータのセキュリティを保ったまま、カード内部でデータのコピーや移動等の処理を行うこと可能にすることにより、電子マネーや個人情報などの重要なデータが外部に漏洩することを防止することが可能な半導体メモリカードを提供することを目的とする。
【課題を解決するための手段】
【０００６】
前記従来の課題を解決するために、本発明の半導体メモリカードは、複数のサービスを提供可能な半導体メモリカードにおいて、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル管理手段と、前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段を備えた。
さらに、本発明の半導体メモリカードでは、前記セキュリティレベル情報取得手段により取得した前記セキュリティレベル情報を出力するセキュリティレベル情報出力手段とを備えた。
さらに、本発明の半導体メモリカードでは、前記セキュリティレベル情報取得手段で取得した前記セキュリティレベル情報を比較し、前記セキュリティレベル情報比較手段で比較した結果により所定のデータ操作処理を行うデータ操作手段を備えた。
また、さらに本発明の半導体メモリカードでは、前記セキュリティレベル情報は、各サービスにおいて取り扱うデータの暗号化条件とした。
また、さらに本発明の半導体メモリカードでは、前記セキュリティレベル情報は、前記サービスを提供するアプリケーションのバージョン番号を含むようにした。
また、さらに本発明の半導体メモリカードでは、前記セキュリティレベル情報比較手段は、比較結果を保存し、該保存した比較結果を参照してセキュリティレベル情報を比較する。
【０００７】
また、本発明の半導体メモリカード処理方法は、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、前記セキュリティレベル情報を取得することを特徴とする。
また、本発明の半導体メモリカード処理プログラムは、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、前記セキュリティレベル情報を取得することを特徴とする。
また、本発明の集積回路は、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル情報管理手段と、前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段とを備えること特徴とする。
【発明の効果】
【０００８】
以上説明したように、複数のサービス間に共通のセキュリティレベル情報と、セキュリティレベル情報を取得するセキュリティレベル情報取得手段とを備えることで、複数のサービスを提供可能な半導体メモリカードを扱う上で、複数サービス間のデータ交換可否を容易に決定することができる。
また、取得したセキュリティレベル情報を出力するセキュリティレベル情報出力手段とを備える構成により、外部ホストにより、複数サービス間のデータ交換可否を容易に決定することができる。

また、取得したセキュリティレベル情報を比較するセキュリティレベル情報比較手段と、比較した結果によりデータ操作処理を行うデータ操作手段を備える構成により、半導体メモリカード内部でデータ処理を完結できるのでセキュリティ機能が高く、ユーザは安心して利用することが可能となる。

また、セキュリティレベル情報を、取り扱うデータの暗号化条件とすることで、データを交換する対象となるサービスもしくは、アプリケーションに対する暗号強度を参照し、暗号強度のより高いサービスもしくは、アプリケーションへのデータ移動は許可し、暗号強度の低いサービスもしくは、アプリケーションへのデータ移動は禁止することにより、データの秘匿性を維持したままデータ交換が可能となる。その結果、ユーザは安心して半導体メモリカードを利用することが可能となる。

また、セキュリティレベル情報にアプリケーションのバージョン番号を含むことで、アプリケーションのアップデートなどの更新情報が反映され、さらにセキュリティ機能を高くすることが可能となる。

また、セキュリティレベル情報比較手段で比較した結果を保存し、保存されている比較結果を参照し、比較することで、認証時間の短縮を図ることができ、ユーザは快適に半導体メモリカードを利用することが可能となる。

【発明を実施するための最良の形態】

【０００９】

以降、本発明にかかる半導体メモリカードの実施形態について説明する。本実施形態にかかる半導体メモリカードは、耐タンパモジュールを内蔵したＩＣカードである。以下本発明の実施の形態について、図面を参照しながら説明する。

【００１０】

（実施の形態１）

まず始めに、本発明に係るＩＣカードの実施行為のうち、使用行為について説明する。ＩＣカード２００は単体、及びポータブルデバイス１２２と接続され、図１に示すような環境でユーザの利用に供される。図１はＩＣカードの使用環境を示す図である。図１における使用環境は、ＥＣサーバ１００、公共サービスサーバ１１０、無線基地局１２０、カードリーダライタ１２１、ポータブルデバイス１２２、ネットワーク１２３から構成される。

【００１１】

ＥＣサーバ１００及び公共サービスサーバ１１０は、無線基地局１２０及びカードリーダライタ１２１、ネットワーク１２３を介してＩＣカード２００にＥＣサービス及び公共サービスを提供する。ＥＣサーバ１００及び公共サービスサーバ１１０には複数のＥＣアプリケーションプログラム（１０１～１０４）及び公共アプリケーションプログラム（１１１～１１３）が動作しており、これらのそれぞれは固有のＥＣサービス及び公共サービスをＩＣカード２００に提供する。ＥＣサーバ１００上で動作するＥＣアプリケーションは、サーバアプリケーションであり、ＥＣサービスの種類毎にそれぞれ異なるものが存在する。

図１では、ｎ種のＥＣサービス毎のＥＣアプリケーションをＥ-ＡＰＬ１、２、・・・ｉ、ｎと略記している。また公共サービスサーバ１１０上で動作する公共アプリケーションもサーバアプリケーションであり、公共サービスの種類毎にそれぞれ異なるものが存在する。図１では、ｎ種の公共サービス毎の公共アプリケーションをＰ-ＡＰＬ１、・・・ｉ、ｎと略記している。

カードリーダライタ１２１は、具体的にはクレジット会社などのキャッシュディスペンサーであり、ＩＣカード２００との入出力を行う。カードリーダライタ１２１はネットワーク１２３と接続されており、このカードリーダライタ１２１を介することでＩＣカード２００は、ＥＣサーバ１００のＥＣサービス及び公共サービスサーバ１１０の公共サービスを受けることが可能である。

【００１２】

無線基地局１２０は建物や電柱の屋上に備え付けの機器であり携帯電話型のポータブル

ータベース１２４と無線によるデータの入出力を行う。無線基地局１２０はネットワーク１２３と接続されており、この無線基地局１２０を介することでもポータブルデバイス１２２はＥＣサーバ１００のＥＣサービス及び公共サービスサーバ１１０の公共サービスを受けることが可能である。

ポータブルデバイス１２２はＩＣカード２００を接続してＩＣカード２００をアクセスする機器である。ポータブルデバイス１２２にはブラウザソフトなどがインストールされており、ユーザはこのブラウザのユーザインタフェースを介して、ＩＣカード２００内のデータにアクセスすることができる。

【００１３】

図２は、一般的なＩＣカード２００のハードウェア構成を示す図である。図２に示すようにＩＣカードにはＣＰＵ２０１、ＲＡＭ２０２、ＲＯＭ２０３、ＥＥＰＲＯＭ２０４、ＩＦ２０５が実装されており、マイコンシステムを形成している。

次にマルチアプリケーション対応のＩＣカードにおけるデータ操作について説明する。図４は、一般的なＩＣカードとホストにおけるデータ操作の概略図である。各アプリケーション単体でのデータ処理は、カードリーダライタ１２１を介して、サーバアプリケーションが行う。カードリーダライタ１２１はポータブルデバイス１２２、基地局１２０であってもよい。

【００１４】

ここでＩＣカード内クライアントＥＣアプリケーションであるＣ-Ｅ-ＡＰＬ１（３０１）のデータを別のＩＣカード内クライアントＥＣアプリケーションであるＣ-Ｅ-ＡＰＬ２（３０２）にコピーあるいは移動する場合について説明する。

まず、サーバ１００内のＥＣサーバアプリケーションＥ-ＡＰＬｉ（１０３）がＥ-ＡＰＬ１（１０１）とＩＣカード内クライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ１（３０１）の認証を行い、次にＥ-ＡＰＬ２（１０２）とＣ-Ｅ-ＡＰＬ２（３０２）の認証を行う。認証処理完了後、Ｅ-ＡＰＬｉ（１０３）はＥ-ＡＰＬ１（１０１）にデータの読み出しを要求し、カードリーダライタ１２１を介してＥ-ＡＰＬ１（１０１）がＩＣカード２００内の対応するクライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ１（３０１）のデータ３３１を読み出す。次に、Ｅ-ＡＰＬｉ（１０３）はＥ-ＡＰＬ２（１０２）にデータの書き込みを要求し、カードリーダライタ１２１を介してＥ-ＡＰＬ２（１０２）がＩＣカード２００内の対応するクライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ２（３０２）にデータ３３２を書き込む。

従って、ＩＣカード内の実データはポータブルデバイスの外へ出る。これは、ＩＣカード内のＯＳにより各アプリケーション用メモリ領域がファイヤウォール３４０で保護されているためである。

【００１５】

次に、本発明のＩＣカードについて説明する。図５は本発明におけるＩＣカードにおけるデータ操作の概略図である。本発明のＩＣカードは、各アプリケーション単体でのデータ処理は一般的なＩＣカードの処理と変わりない（図４参照）。また、カードのハードウェア構造は一般的なＩＣカードのハードウェア構造（図２）と変わりない。

図６は本発明の基本となるマルチアプリケーション対応のＩＣカードのソフトウェア構成を示した図である。アプリケーション用メモリ領域３１０、ＯＳ３１１、クライアントＥＣアプリケーション３０１と、クライアントＥＣアプリケーション３０２、とを備えている点は一般的なＩＣカードと変わりない。

しかし、本発明では複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル定義情報６００と、ＩＣカード内に格納されているアプリケーションを管理するためのアプリケーション情報管理テーブル６０１と、前記セキュリティレベル情報とアプリケーション情報管理テーブルを管理するセキュリティレベル情報管理手段６０２と、前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段６０４と、前記セキュリティレベル情報取得手段により取得した前記セキュリティレベル情報を出力するセキュリティレベル情報出力手段６０５と、前記セキュリティレベル

情報出力手段により出力されたセキュリティレベル情報をサーバで比較するサーバ側セキュリティレベル情報比較手段６０７と、前記セキュリティレベル情報出力手段により出力されたセキュリティレベル情報をカード内で比較するクライアント側セキュリティレベル情報比較手段６０６と、前記セキュリティレベル情報比較手段で比較した結果を基に、所定のデータ操作処理を行うデータ操作手段６０８、とを備えている点が異なる。

【００１６】

セキュリティレベル定義情報６００は、セキュリティレベルの高低により異なる条件を含む（図７）。例えば、値が０３ｈの場合はセキュリティレベルが“高”であり、データをＴｒｉｐｌｅ－ＤＥＳ方式で暗号化する。次に値が０２ｈの場合はセキュリティレベルが“中”であり、データをＤＥＳ方式で暗号化する。さらに値が０１ｈの場合はセキュリティレベルが“低”であり、データをＡＥＳ方式で暗号化する。値が００ｈの場合はセキュリティレベルが“なし”であり、データを暗号化しない、という条件である。

アプリケーション情報管理テーブル６０１は、ＩＣカード内に格納されている各アプリケーションに関する情報を保持している（図８）。アプリケーションに関する情報とは、例えば、アプリケーションを識別するためのアプリケーションＩＤ、前記セキュリティレベル定義情報６００で定義されたセキュリティレベル、暗号鍵のビット長である暗号情報、暗号鍵、アプリケーションのバージョン情報などである。図８では、クライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ１（３０１）は、アプリケーションＩＤが３４１２ｈ、セキュリティレベルが０１ｈ（低）、暗号鍵ビット長が８０ｈ、暗号鍵が１２８ｂｉｔ（１６ｂｙｔｅ）分、バージョン情報が０１ｈであることを示しており、クライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ２（３０２）は、アプリケーションＩＤが７８５６ｈ、セキュリティレベルが０３ｈ（高）、暗号鍵ビット長がＣ０ｈ、暗号鍵が１９２ｂｉｔ（２４ｂｙｔｅ）分、バージョン情報が０５ｈであることを示しており、クライアント公共アプリケーションＣ-Ｐ-ＡＰＬ１（３０３）は、アプリケーションＩＤがＦＦＦＥｈ、セキュリティレベルが０２ｈ（中）、暗号鍵ビット長が４０ｈ、暗号鍵が６４ｂｉｔ（８ｂｙｔｅ）分、バージョン情報が１Ａｈであることを示している。

【００１７】

以下、図９において、データ操作要求において操作が完了するまでの手順を示すフローチャートを参照し、本発明のＩＣカードの動作について詳細に説明を行う。

まず、処理要求発生後ＥＣサーバ１００のサーバアプリケーションＥ-ＡＰＬｉ（１０３）はサーバアプリケーションＥ-ＡＰＬ１（１０１）の認証をＩＣカード内のクライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ１（３０１）に対して行い（Ｓ９０１）、次にＥ-ＡＰＬ１（１０１）に対応するＥ-ＡＰＬ２（１０２）の認証もクライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ２（３０２）に対して行う（Ｓ９０２）。各アプリケーション認証完了後、ユーザはデータ操作したいデータを選択する（Ｓ９０３）。

その後、セキュリティレベル情報取得手段６０４はアプリケーションＩＤを元に、セキュリティレベル情報管理手段６０２からクライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ１（３０１）及びＣ-Ｅ-ＡＰＬ２（３０２）のセキュリティレベル情報を取得する（Ｓ９０４）。次に、セキュリティレベル情報出力手段６０５は取得したセキュリティレベル情報を出力し（Ｓ９０５）、ＩＣカード２００はＥＣサーバ１００に対して、セキュリティレベル情報を含むレスポンスを返す。さらに、ＥＣサーバ１００内のサーバ側セキュリティレベル情報比較手段６０７は、出力されたセキュリティレベル情報を比較し、条件を満たす場合は、ＩＣカード２００にデータ操作をＩＣカード内部で実行するよう要求（ＡＰＤＵコマンド）を送信する（Ｓ９０６）。そして、ＩＣカード２００ではデータ操作手段６０８は出された要求やアプリケーションＩＤ、ファイルＩＤなどのデータ操作情報を元に、選択されたＣ-Ｅ-ＡＰＬ１（３０１）のデータをＣ-Ｅ-ＡＰＬ２（３０２）にコピーする処理を実行する（Ｓ９０７）。

ここで、条件を満たさない場合はＩＣカード外部つまりＥＣサーバ１００を介して操作を実行することをユーザに確認し（Ｓ９０９）、処理続行であれば、サーバを介して処理を実行する（Ｓ９１０）。処理完了後、処理を続行する場合は、処理データの選択（Ｓ９

ＳＯＳ）に戻ることとする。

【００１８】

具体的に、ユーザがクライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ１（３０１）に格納されている氏名、住所、電話番号などの個人情報をクライアントＥＣアプリケーションＣ-Ｅ-ＡＰＬ２（３０２）にコピーしたい場合についての例を示す。

ユーザはポータブルデバイス１２２やカードリーダライタ１２１等の表示画面でＣ-Ｅ-ＡＰＬ１（３０１）及びＣ-Ｅ-ＡＰＬ２（３０２）を選択する。これによりＩＣカード２００は各アプリケーションの認証を実行する（Ｓ９０１、Ｓ９０２）。その後、表示画面でコピー処理を実行したいデータ（ここでは、氏名、住所、電話番号とする）の選択を行う（Ｓ９０３）。データ選択完了後ＩＣカード２００では、セキュリティレベル情報取得手段６０４を用いて、指定された各アプリケーションのセキュリティレベル情報を取得し（Ｓ９０４）、取得したセキュリティレベル情報をＥＣサーバ１００にレスポンスとして送信する（Ｓ９０５）。ＥＣサーバ１００は出力されたセキュリティレベル情報を元に各サービスのレベルの比較を行う。ここで、Ｃ-Ｅ-ＡＰＬ１（３０１）のセキュリティレベル情報は値が０１ｈであるため、レベル“低”であり、Ｃ-Ｅ-ＡＰＬ２（３０２）のセキュリティレベルは値が０３ｈであるためレベル“高”となる。従って、コピー元（Ｃ-Ｅ-ＡＰＬ１（３０１））のセキュリティレベルのほうが低レベルであるため、ＩＣカード２００にカード内で処理を行うよう要求し、セキュリティレベルが“低”であるＣ-Ｅ-ＡＰＬ１（３０１）から、セキュリティレベルが“高”であるＣ-Ｅ-ＡＰＬ２（３０２）へ、カード内でのコピー処理が可能となる（Ｓ９０７）。コピー処理完了後、表示画面に処理を続行するかとうかの選択画面が現れるため、ユーザは他のデータのコピーを実行したいのであれば、他のデータを選択することが可能となる。

【００１９】

以上、セキュリティレベルが“低”であるようなアプリケーションから、セキュリティレベルが“高”であるようなアプリケーションに対するデータコピーないし移動は、特別な指示がなくても可能であるが、逆に、セキュリティレベルが“高”であるようなアプリケーションから、セキュリティレベルが“低”であるようなアプリケーションに対するデータコピーないし移動は、データの秘匿性の維持の観点からユーザに対する警告を行ってデータコピーないし移動をするか、それを禁止することが望ましい。かかる構成によれば、各サービスに共通のセキュリティレベル定義情報を持ち、各サービスのセキュリティレベル情報を取得し、取得したセキュリティレベル情報を出力し、出力されたセキュリティレベル情報をサーバで比較し、条件を満たす場合はカード内部でデータ操作を行うことが可能となり、利用者はデータが外部に漏洩する危険性を有することなく異なるサービス間のデータ操作を完了することができる。

【００２０】

（実施の形態２）

第１の実施形態では、セキュリティレベル情報の比較をサーバアプリケーションであるＥ-ＡＰＬｉ（１０３）で行っていたが、本発明はこれに限定されるものではなく、ＩＣカード内部で比較する場合も考えられる。そこで、第２実施形態では、ＩＣカード内にクライアント側セキュリティレベル情報比較手段６０６を備えた場合を示すこととする。

図１０のフローチャートを参照し、本発明のＩＣカードの動作について説明を行う。基本的な処理の流れは、第１実施形態と変わりない。しかし、クライアント側セキュリティレベル情報比較手段６０６をＩＣカード内部に備えることで、取得したセキュリティレベル情報を外部に出すことなく比較する（Ｓ１００５）ことが可能となる点が異なる。

また、第１実施形態では、セキュリティレベル情報を“高”、“中”、“低”、“なし”、としていたが、第２実施形態ではセキュリティレベル情報を、各サービスの実データ等を暗号化するための暗号化条件、例えば、鍵長、鍵データ、暗号化方式とすることも特徴とする。

この場合、セキュリティレベル情報の比較をサーバで行うと、各アプリケーションに対応する暗号化条件が外部に漏洩し、実データが改ざんされる可能性があるため、第２実施

形態を取ることで、重要なデータの漏洩を防ぐことが可能となる。

【００２１】

（実施の形態３）

第２の実施形態では、セキュリティレベル情報を各サービスの実データ等を暗号化するための暗号化条件としていたが、第３実施形態では、セキュリティレベル情報にはアプリケーションプロトコルのバージョンを含むことも特徴とする。

従来、ＩＣカード２００とサーバ１００、１１０（カードリーダライタ１２１）では図１１に示すアプリケーションプロトコルデータユニット（ＡＰＤＵ）コマンドを使用してデータの送受信が行われている。そこで、ＡＰＤＵコマンドのヘッダ部分である制御パラメータ（Ｐ１、Ｐ２）を用いてアプリケーションプロトコルバージョンをコマンドに付加することも特徴とする。

一般に、アプリケーションプロトコルは機能拡張されるにしたがってその、バージョン番号を上げて定義される。例えば、セキュリティ上の拡張または、改良を加えた結果バージョン番号が上ることがある。その場合、プロトコルバージョンを比較して、より上位バージョンのプロトコルの方がセキュリティ強度が高いといえる。

【００２２】

以下、図１２以降の図を用いて、ＡＰＤＵコマンドにアプリケーションプロトコルバージョンを付加する場合について説明する。

図１２はＩＳＯ７８１６で規定されており、金融系で使用されているコマンドを示している。例えば図１３に示すようにＳＥＬＥＣＴコマンドの場合、Ｐ１に未使用ビットが存在する（ｂ８～ｂ４）。この未使用の５ビットを用いることで、０から３１までの値が設定可能となる。

また、図１４に示すようにクラスバイト（ＣＬＡ）のｂ８を１に設定することで固有コマンドが使用可能となるが、これを用いることでＰ１の１バイトを全てプロトコルバージョンに割り当てることも可能となり、この場合０から６５５３５までの値が設定可能となる。

例えば、Ｃ-Ｅ-ＡＰＬ１（３０１）からＣ-Ｅ-ＡＰＬ２（３０２）にデータをコピーしたい場合、Ｃ-Ｅ-ＡＰＬ１（３０１）のプロトコルバージョンは０１ｈであり、Ｃ-Ｅ-ＡＰＬ２（３０２）のプロトコルバージョンは０５ｈであるため、比較結果Ｃ-Ｅ-ＡＰＬ２（３０２）のプロトコルバージョンが上位であり、セキュリティ強度が高いと判断できるため、データコピー処理の実行が可能となる。

以上説明したように、ＡＰＤＵコマンドにアプリケーションプロトコルバージョンを付加することで、アプリケーションごとのプロトコルバージョンを取得し、比較することが可能となり、コピー先のアプリケーションプロトコルバージョンがコピー元のアプリケーションプロトコルバージョンより古いバージョンの場合は、通信セキュリティレベルが落ちると判断しデータコピーなどの処理を不可とすることが可能となり、データ漏洩の危険性が減少することとなる。

【００２３】

（実施の形態４）

さらに、第１の実施形態において、サーバ内のアプリケーションで、出力されたセキュリティレベル情報を比較していたが、本発明はこれに限定されるものではなく、比較した結果を保存しておく場合も考えられる。この場合、同一アプリケーション間での認証、及び比較をデータ操作の度に行う必要が無く、処理時間の短縮が図られることとなる。

【００２４】

（実施の形態１～実施の形態４の第１の補足事項）

以上、実施形態１、２、３、４を説明した。尚、これまでの説明において本発明のＩＣカードにおいて備えている、セキュリティレベル情報管理手段、セキュリティレベル情報取得手段、セキュリティレベル情報出力手段、セキュリティレベル情報比較手段、データ操作手段等は、コンピュータプログラムとして実現される。当該プログラムは、ＩＣカード内のＲＯＭに格納され実行されるものと、外部よりダウンロードされ、不揮発性メモリ

に格納され実行されるものとがある。

【００２５】

（実施の形態１～実施の形態４の第２の補足事項）

また、さらに、上述の機能ブロックは、ＣＰＵ、ＲＡＭ、ＲＯＭ、不揮発性メモリ等のハードウェア資源との組み合わせにより、集積回路であるＬＳＩとして実現される場合がある。これらは、個別に１チップ化されても良いし、一部又はすべてを含むように１チップ化されても良い。

図１５に実施の形態１、実施の形態２、実施の形態３における集積回路化の一例を示す。ＬＳＩ２０００は集積回路化の一例を示し、集積回路化する機能ブロックの範囲の例である。ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製作後にプログラムすることが可能なＦＰＧＡ(Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ)やＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

【産業上の利用可能性】

【００２６】

本発明にかかる半導体メモリカードは、カード内のアプリケーションのみでデータ交換が可能であるため、複数のサービスを提供可能かつデータの保護機能に優れた半導体メモリカード等として有用である。

【図面の簡単な説明】

【００２７】

【図１】一般的なＩＣカードの利用形態概観図

【図２】一般的なＩＣカードのハードウェア構成図

【図３】一般的な複数サービス対応のＩＣカードのソフトウェア構成図

【図４】一般的な複数サービス対応ＩＣカードのデータ処理（コピー、移動）概略図

【図５】本発明の基本となる複数サービス対応ＩＣカードのデータ処理（コピー、移動）概略図

【図６】本発明のソフトウェア構成図

【図７】セキュリティレベル定義情報構成図

【図８】アプリケーション情報管理テーブル構成図

【図９】本発明のデータ処理手順フローチャート１

【図１０】本発明のデータ処理手順フローチャート２

【図１１】アプリケーションプロトコルデータユニット構成図

【図１２】全産業共通コマンド例を示す図

【図１３】ＳＥＬＥＣＴコマンドにおける制御パラメータ１を示す図

【図１４】命令クラスバイトを示す図

【図１５】実施の形態１、実施の形態２、実施の形態３における集積回路化の一例を示す図

【符号の説明】

【００２８】

１００　ＥＣサーバ

２００　ＩＣカード

３０１　クライアントＥＣアプリケーション１

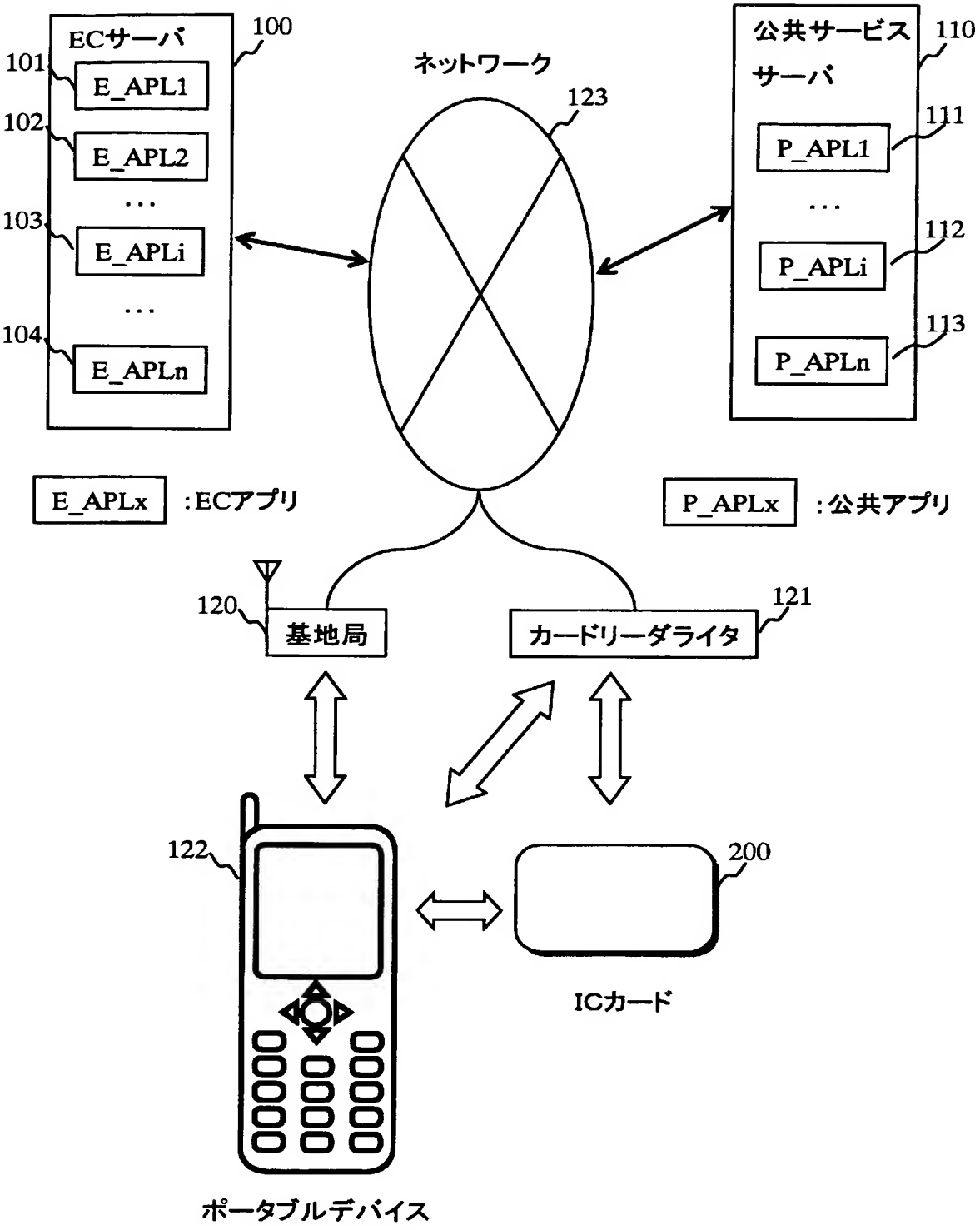
３０２　クライアントＥＣアプリケーション２

３１０　アプリケーション用メモリ領域

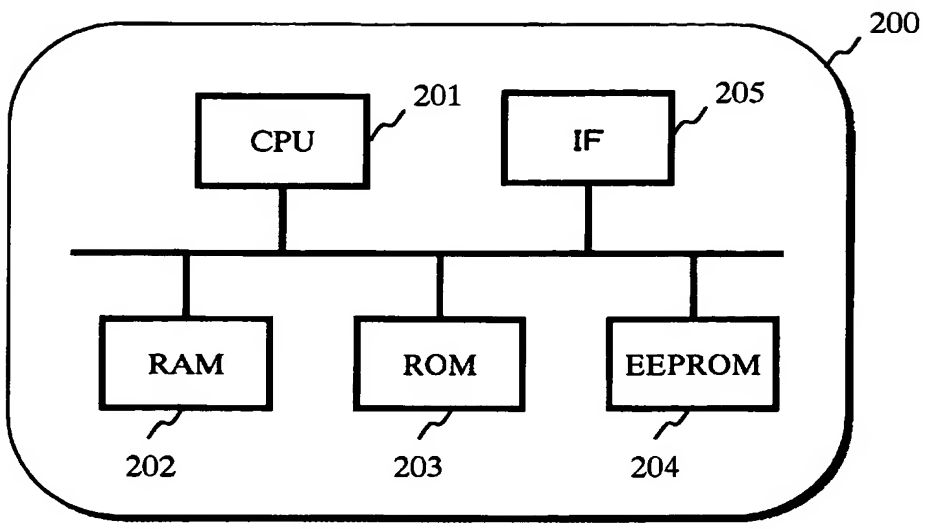
３３１　アプリケーション１内データ領域（複写元）

３３２　アプリケーション毎データ領域（後半分）
６００　セキュリティレベル定義
６０１　アプリケーション情報管理テーブル
６０２　セキュリティレベル情報管理手段
６０３　セキュリティレベル情報設定手段
６０４　セキュリティレベル情報取得手段
６０５　セキュリティレベル情報出力手段
６０６　クライアント側セキュリティレベル情報比較手段
６０７　サーバ側セキュリティレベル情報比較手段
６０８　データ操作手段

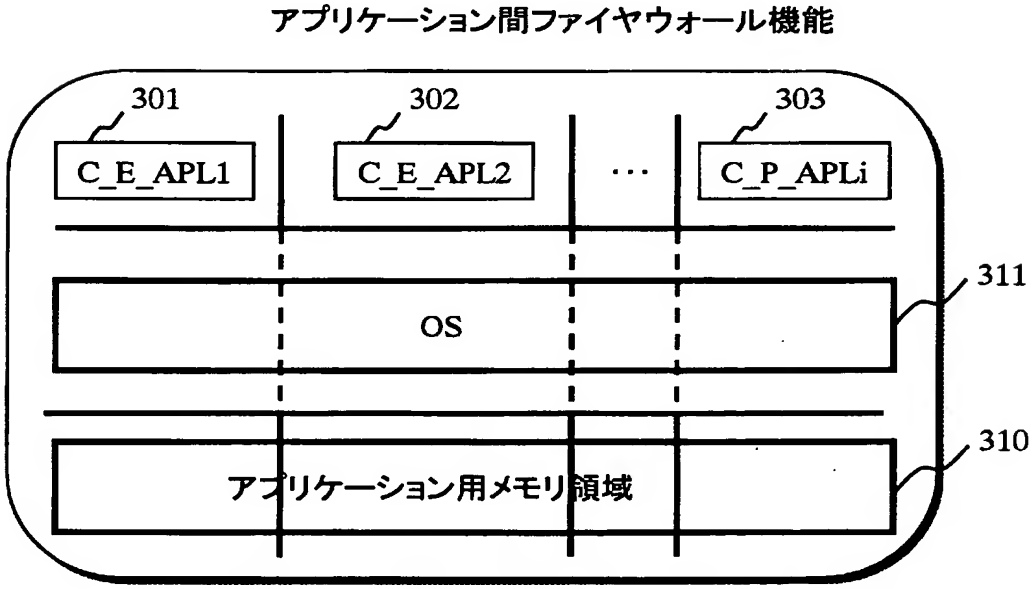
【書類名】図面
【図１】


ECサーバ
100
101
E_APL1
102
E_APL2
...
103
E_APLi
...
104
E_APLn
ネットワーク
123
公共サービス
サーバ
110
111
P_APL1
...
112
P_APLi
113
P_APLn
E_APLx
:ECアプリ
P_APLx
:公共アプリ
120
基地局
121
カードリーダライタ
122
200
ICカード
ポータブルデバイス

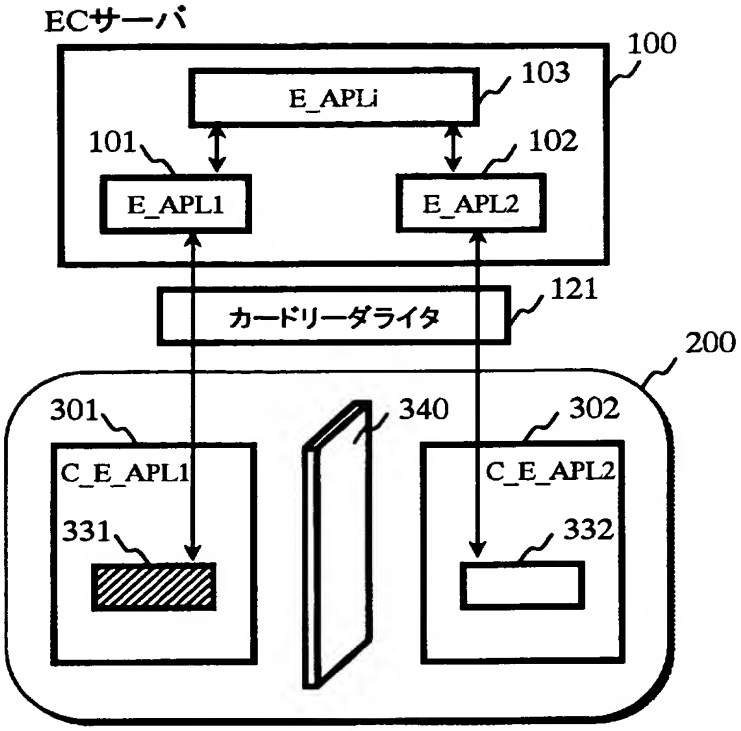
【図２】


ICカード
200
CPU
201
IF
205
RAM
ROM
EEPROM
202
203
204

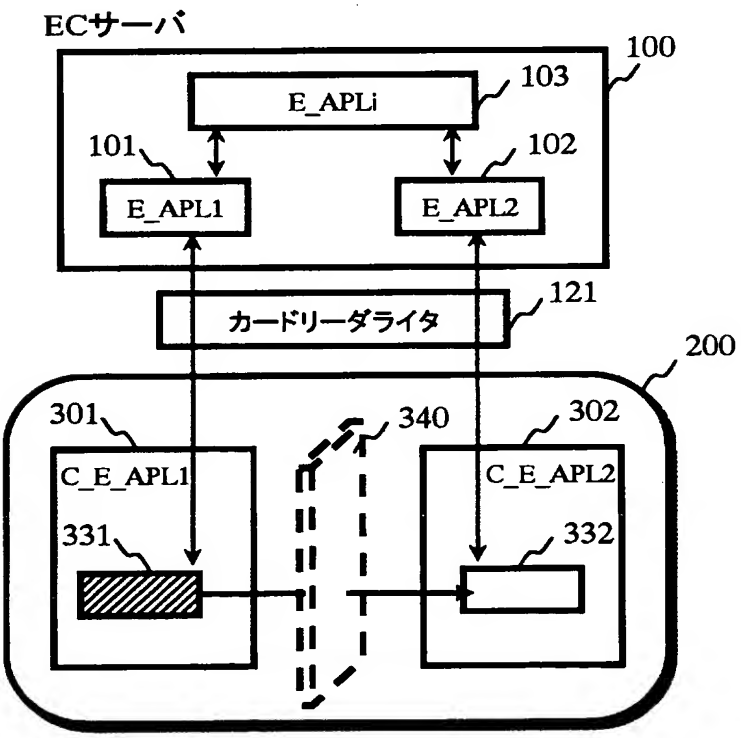
【図３】

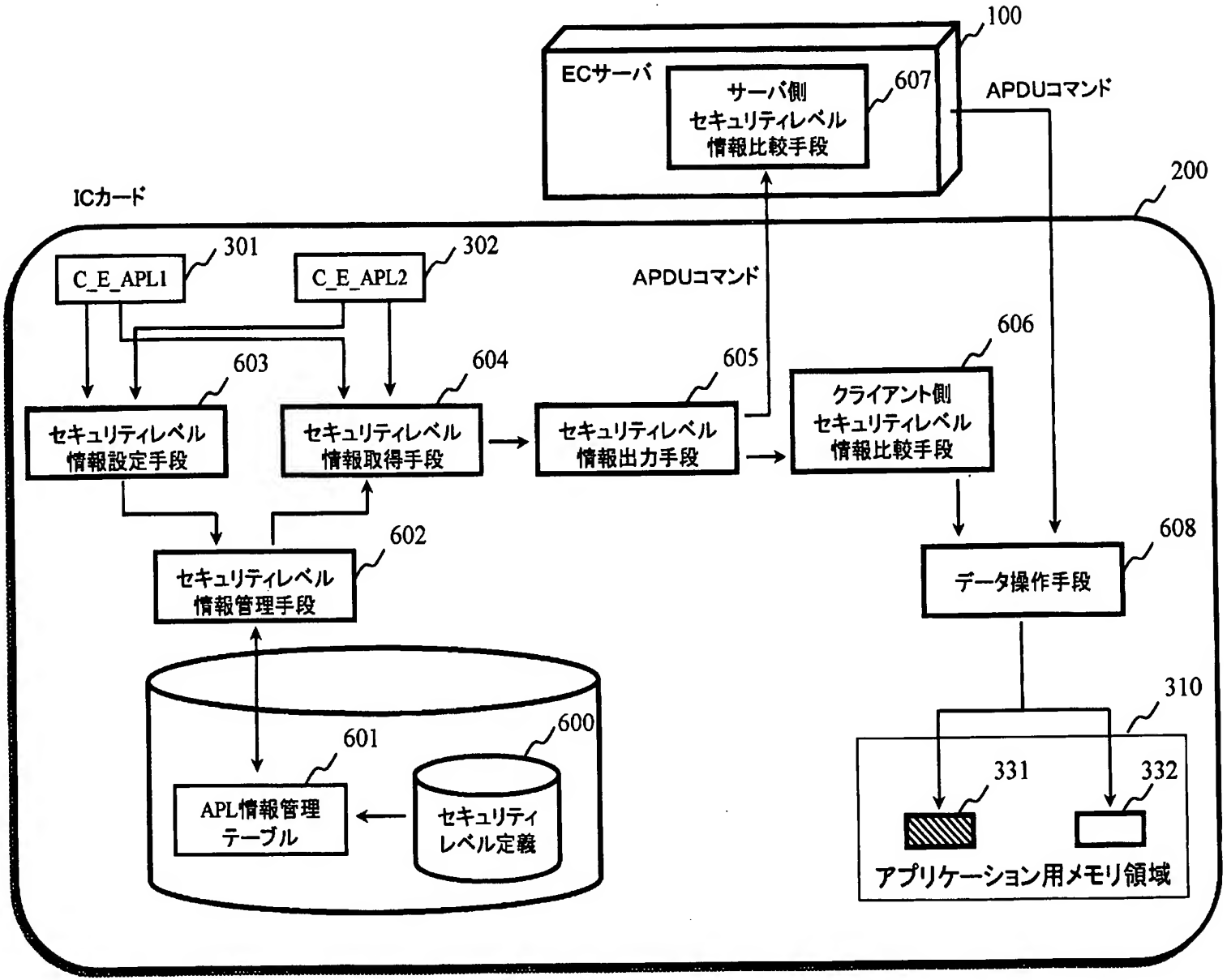

アプリケーション間ファイヤウォール機能
301
302
303
C_E_APL1
C_E_APL2
・・・
C_P_APLi
OS
311
アプリケーション用メモリ領域
310

【図４】

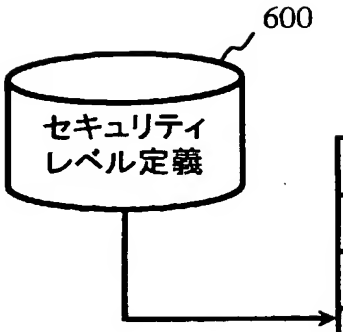

ECサーバ
100
E_APLi
103
101
102
E_APL1
E_APL2
121
カードリーダライタ
200
301
340
302
C_E_APL1
C_E_APL2
331
332

【図５】


ECサーバ
100
E_APLi
103
101
102
E_APL1
E_APL2
121
カードリーダライタ
200
301
340
302
C_E_APL1
C_E_APL2
331
332

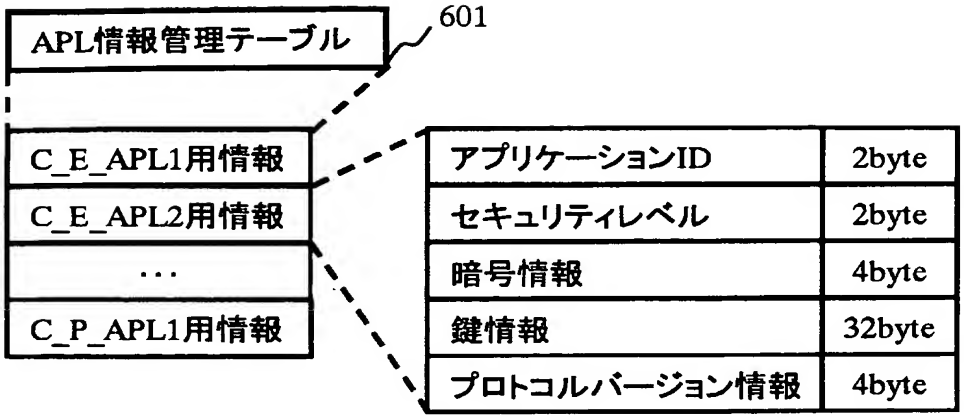

100
ECサーバ
サーバ側
セキュリティレベル
情報比較手段
607
APDUコマンド
200
ICカード
301
C_E_APL1
302
C_E_APL2
APDUコマンド
606
603
604
605
セキュリティレベル
情報設定手段
セキュリティレベル
情報取得手段
セキュリティレベル
情報出力手段
クライアント側
セキュリティレベル
情報比較手段
602
608
セキュリティレベル
情報管理手段
データ操作手段
310
601
600
331
332
APL情報管理
テーブル
セキュリティ
レベル定義
アプリケーション用メモリ領域

【図７】



700

レベル	値	レベルの基準
高	03h	Triple-DES暗号方式
中	02h	DES暗号方式
低	01h	AES暗号方式
なし	00h	暗号なし



C_E_APL1用情報

アプリケーションID	12h	34h				
セキュリティレベル	01h	00h				
暗号情報	80h	00h	00h	00h		
鍵情報	01h	02h	03h	・・・	00h	00h
バージョン情報	01h	00h	00h	00h		

C_E_APL2用情報

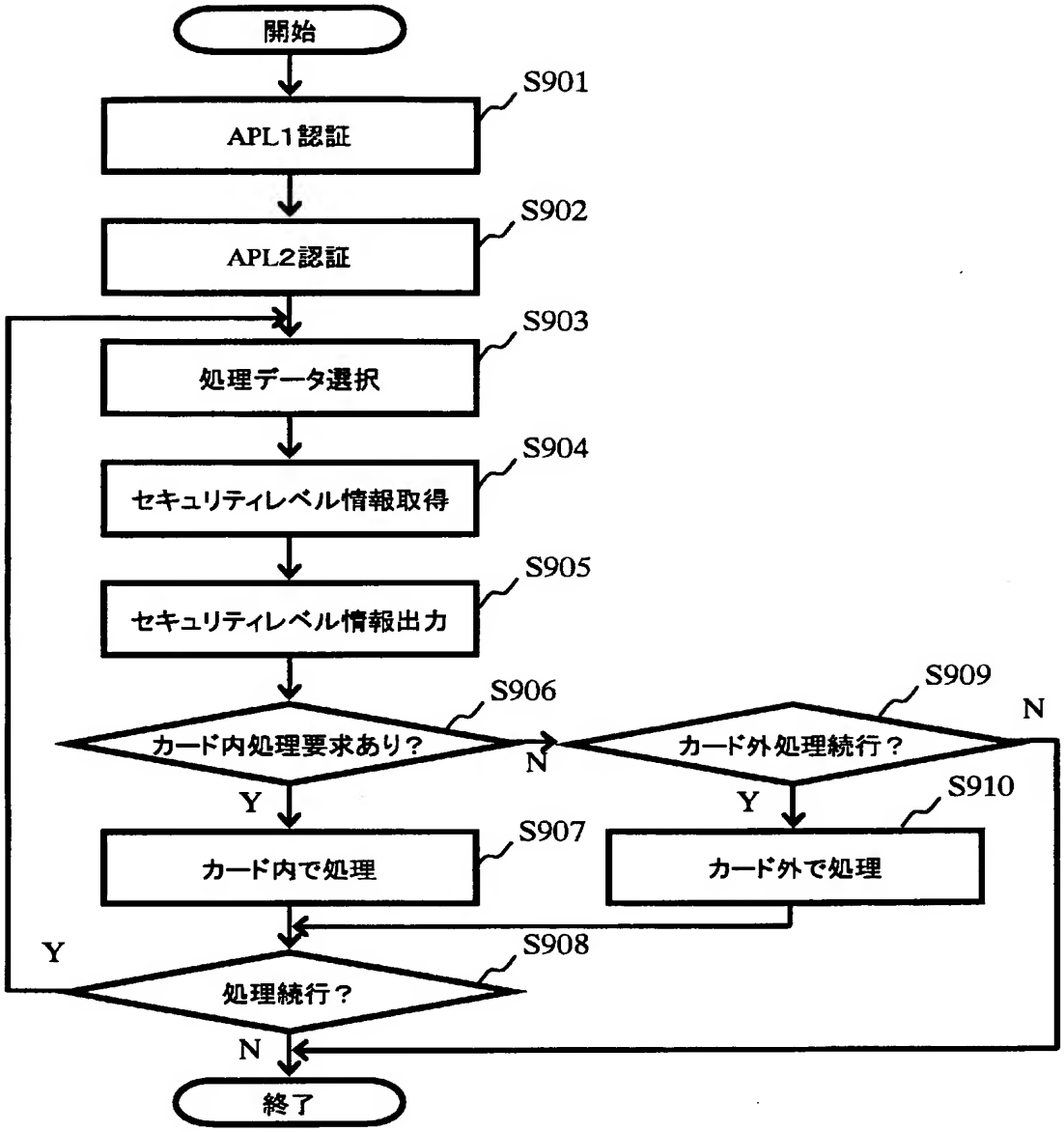
アプリケーションID	56h	78h				
セキュリティレベル	03h	00h				
暗号情報	C0h	00h	00h	00h		
鍵情報	FFh	FEh	FDh	・・・	00h	00h
バージョン情報	05h	00h	00h	00h		

・・・

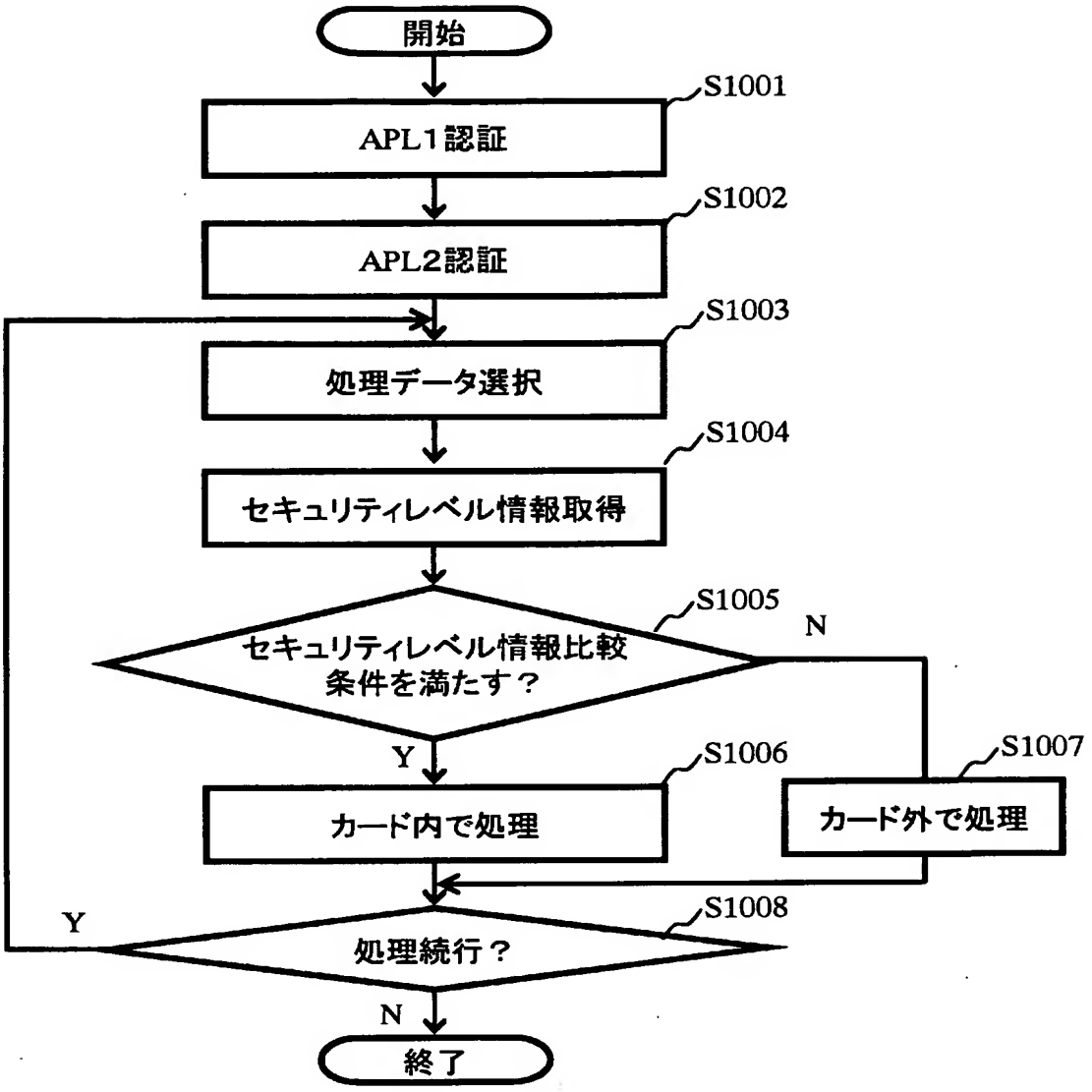
C_P_APL1用情報

アプリケーションID	FEh	FFh				
セキュリティレベル	02h	00h				
暗号情報	40h	00h	00h	00h		
鍵情報	11h	22h	33h	・・・	00h	00h
バージョン情報	1Ah	00h	00h	00h		

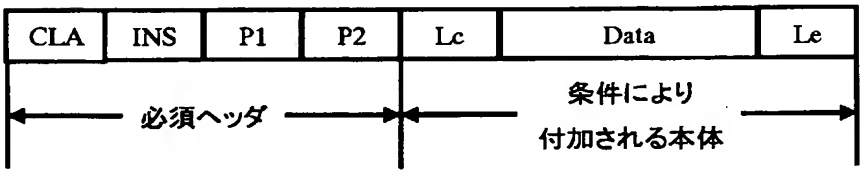
【図９】


開始
S901
APL1認証
S902
APL2認証
S903
処理データ選択
S904
セキュリティレベル情報取得
S905
セキュリティレベル情報出力
S906
カード内処理要求あり？
N
Y
S907
カード内で処理
S909
カード外処理続行？
N
Y
S910
カード外で処理
S908
処理続行？
Y
N
終了

【図１０】


開始
S1001
APL1認証
S1002
APL2認証
S1003
処理データ選択
S1004
セキュリティレベル情報取得
S1005
セキュリティレベル情報比較
条件を満たす？
N
Y
S1006
カード内で処理
S1007
カード外で処理
S1008
Y
処理続行？
N
終了

【図１１】


CLA
INS
P1
P2
Lc
Data
Le
必須ヘッダ
条件により
付加される本体

【図１２】

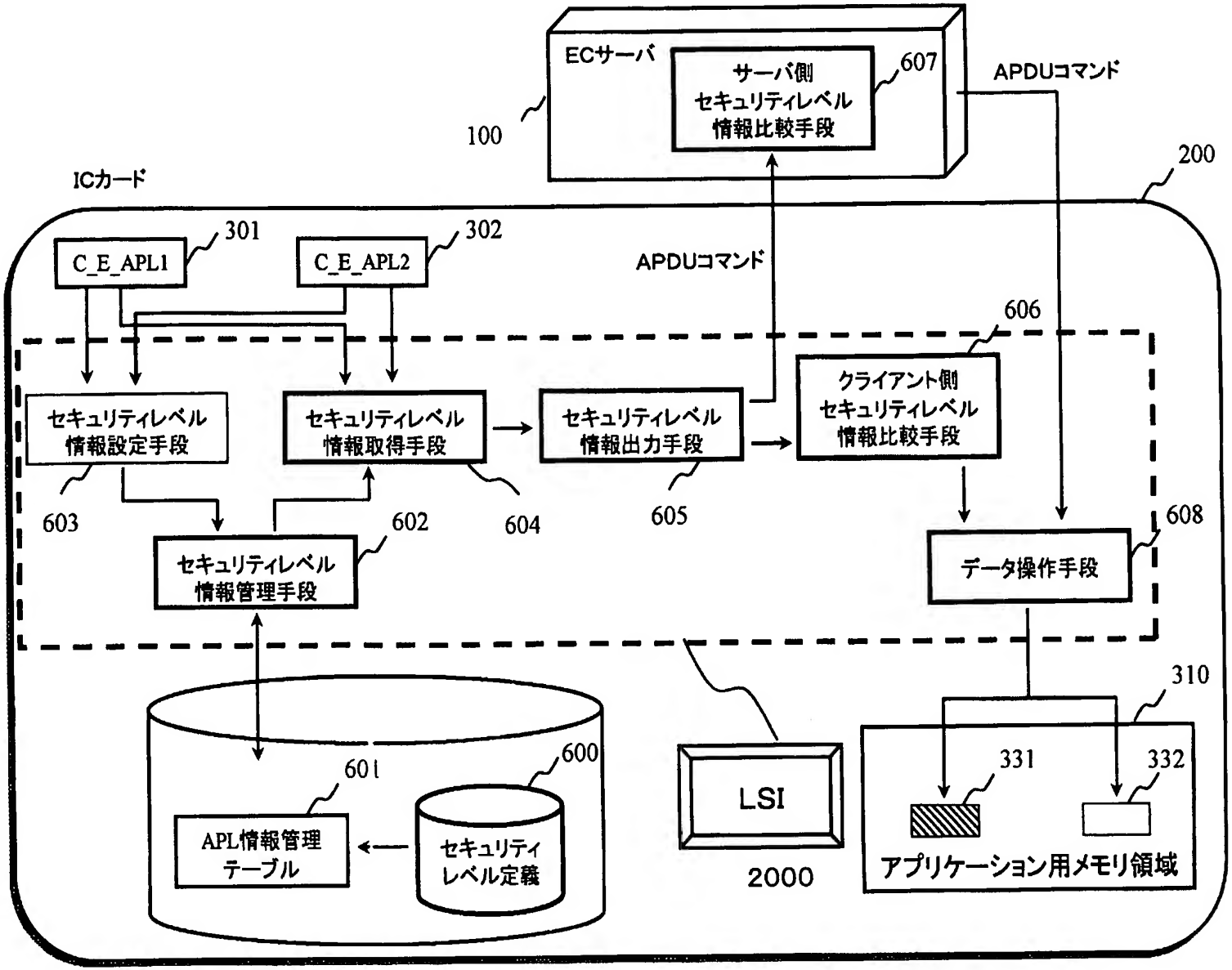
コマンド名	SELECT	READ RECORD	INTERNAL AUTHENTICATE
CLA(1byte)	00h	00h	00h
INS(1byte)	A4h	B2	88h
P1(1byte)	XXh	レコード番号	00h
P2(1byte)	00h	XXh	00h

【図１３】

b8	b7	b6	b5	b4	b3	b2	b1	意味
x	x	x	x	x				未使用
					1			名前による選択
						0	0	

【図１４】

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0					全産業共通コマンド
1	0	0	0					独自コマンド


ECサーバ
サーバ側
セキュリティレベル
情報比較手段
607
APDUコマンド
100
200
ICカード
301
C_E_APL1
302
C_E_APL2
APDUコマンド
606
セキュリティレベル
情報設定手段
セキュリティレベル
情報取得手段
セキュリティレベル
情報出力手段
クライアント側
セキュリティレベル
情報比較手段
603
602
604
605
608
セキュリティレベル
情報管理手段
データ操作手段
310
601
600
LSI
331
332
APL情報管理
テーブル
セキュリティ
レベル定義
2000
アプリケーション用メモリ領域

【書類名】要約書

【要約】

【課題】ＩＣカード内のデータをカード外部に読み出すことなくデータ交換を行うことが可能なＩＣカードを提供すること。

【解決手段】セキュリティレベル定義情報６００と、アプリケーション情報管理テーブル６０１と、セキュリティレベル情報管理手段６０２と、セキュリティレベル情報取得手段６０４と、セキュリティレベル情報出力手段６０５と、クライアント側セキュリティレベル情報比較手段６０６と、データ操作手段６０８、とを備え、ＩＣカード内でデータ操作が完結するため、ユーザは個人情報などの重要なデータが外部に漏洩する危険性を有することなくＩＣカードを利用することが可能となる。

【選択図】図６

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006805

International filing date: 31 March 2005 (31.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-114330
Filing date: 08 April 2004 (08.04.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse